UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/898,286	07/03/2001	Geoffrey Donald Tremain	1821-01100	2215

23505 7590 03/23/2007

CONLEY ROSE, P.C.
P. O. BOX 3267
HOUSTON, TX 77253-3267

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	PAPER NUMBER
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/898,286	TREMAIN, GEOFFREY DONALD	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 March 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-64* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-64* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Pre-Appeal brief request for review was filed on March 08, 2007. The Office has reopened the prosecution in view of new grounds of rejection(s).

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-36, and 56-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wesinger, JR. et al. herein after (Wesinger) Pub. No. US 2001/0011304 A1 in view of Rogers et al. USPN 5,701,451.

Regarding claims 1, and 20, Wesinger discloses an apparatus/method of providing for a plurality of customers (0012 lines 7-8, and 0050; *web users ... remote hosts*) one or more computer services selected from: file, data and archiving services; applications hosting services; database hosting services; data warehouse services; knowledge management hosting services; digital media production services; "intellectual property" and streaming media services; simple web hosting services; complex e-Commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services (0035; *web hosting services*); the method comprising the steps of:

setting up on a real computer (fig. 1; *web server physical machine*) at the request of each of said customers (0024 and 0026; *user connection request to connect and access...*) at least one virtual machine (fig. 1 *virtual host 1, 2, ... N*) for each of said customers, said at least one virtual machine for each of said customers having a specification determined in accordance with the computer service or services requested by said customer and being configurable by said customer (0035 and 0045-0053; *configuring multiple virtual hosts and/or client computers based on users preferences/budgets*).

Wesinger fails to disclose said at least one virtual machine having a separate operating system running thereon.

However Rogers et al. discloses a World Wide Web server providing web requests to client and an operating system that enables multiple kinds of operating systems, including "UNIX" to co-exist on a single platform (see col. 6 lines 39-44).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Rogers et al. within the system of Wesinger because they are analogous in service providing. One would have been motivated to incorporate the teachings of Rogers et al. because it would fulfill users request as an agent of the browser client without transmitting users request to another server to provide access to the user.

Regarding claims 2 and 21, Wesinger further teaches an apparatus/method, wherein plural virtual machines are set up within the real computer for at least one of said customers (fig. 1; *web server physical machine and VH1... VHN*).

Regarding claims 3 and 22, Wesinger further teaches an apparatus/method, wherein the or each virtual machine for at least one of said customers is connected to a virtual network set up for said at least one customer within the real computer (0021-0027).

Regarding claims 4 and 23, Wesinger further teaches an apparatus/method, comprising a virtual intrusion detection device for detecting an attack on the virtual network (The examiner takes an official notice on virtual intrusion detection as a well-known at the time of the invention was made because it would enable secure virtual network (see, Cisco News Release by San Jose pages 4-5).

Regarding claims 5 and 24, Wesinger further teaches an apparatus/method, wherein at least one virtual machine is connected to a virtual firewall that is connectable to an external network to which customers and/or other users can connect such that access to said at least one virtual machine by a customer or other user via a said external network can only take place through a virtual firewall (0025).

Regarding claims 6 and 25, Wesinger further teaches an apparatus/method, wherein the or each virtual machine for a particular customer is connected to a virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall being connectable to an external network to which each of said customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall provided for that virtual machine or machines (0039).

Regarding claims 7 and 26, Wesinger further teaches an apparatus/method, wherein each virtual firewall is set up within the real computer, the or each virtual machine for each customer being connected to a first port of the virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall having a second port connected to a virtual network that is set up within the real computer and that is connectable to an external network (0039).

Regarding claims 8 and 27, Wesinger further teaches an apparatus/method, wherein the second port of each virtual firewall is connected to the same virtual network that is set up within the real computer and that is connectable to an external network (0025).

Regarding claim 9, Wesinger further teaches an apparatus/method, wherein the or at least one of the virtual firewalls is implemented by a virtual machine on the real computer, said virtual firewall virtual machine running firewall software (0039).

Regarding claims 10 and 28, Wesinger further teaches an apparatus/method, comprising a plurality of real data storage devices and at least one virtual storage subsystem that is configured to allow said real data storage devices to emulate one or more virtual storage devices (0026).

Regarding claims 11 and 29, Wesinger further teaches an apparatus/method, wherein the at least one virtual storage subsystem is configured to emulate at least one respective virtual storage device for each customer (0026).

Regarding claims 12 and 30, Wesinger further teaches an apparatus/method, comprising a detection device for detecting evidence of malicious software or hostile attack signatures on the at least one virtual storage subsystem (0025).

Regarding claims 13 and 31, Wesinger further teaches an apparatus/method, wherein the apparatus is configurable to provide at least one of the services selected from: file, data and archiving services; applications hosting services; database hosting services; data warehouse services; knowledge management hosting services; digital media production services; "intellectual property" and streaming media services; simple web hosting services; complex e-Commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services (0035).

Regarding claims 14 and 32, Wesinger further teaches an apparatus/method, comprising virtual private network software to provide an encrypted communication channel for communication between at least some of said virtual machines (0053).

Regarding claims 15 and 33, Wesinger further teaches an apparatus/method, comprising virtual private network software to provide an encrypted communication channel for communication between at least one virtual machine and an external computer (0021-0024).

Regarding claims 16 and 34, Wesinger further teaches an apparatus/method, comprising virtual

private network software to provide an encrypted communication channel for communication between a first virtual network and a second virtual network (0053).

Regarding claims 17 and 35, Wesinger further teaches an apparatus/method, comprising virtual private network software to provide an encrypted communication channel for communication between a virtual network and an external computer (0021-0026).

Regarding claim 18, Wesinger further teaches an apparatus/method, wherein the real computer comprises plural physical computers (fig. 1).

Regarding claim 19, Wesinger further teaches in combination, a first apparatus according to claim 1 and a second apparatus that is substantially identical to said first apparatus, the first and second apparatus being connected by a communications channel so that the second apparatus can provide for redundancy of the first apparatus thereby to provide for disaster recovery if the first apparatus fails (The Examiner takes an official notice wherein second apparatus for providing disaster recovery if the first apparatus/real computer fails. It is well known in the art at the time of the invention to have a backup server to recover a disaster when failure of a host server because it would provide an efficient service with out failing to provide user requests during power outage/system failure (see, Seagate software press releases 1997 pages 1-2).

Regarding claim 36, Wesinger further teaches the method, comprising the step of moving said at least one virtual machine from a first real computer to a second real computer (The Examiner

takes an official notice again because to backup data during system failure the step of moving is necessary because it would recover data (see, Seagate software press releases 1997 pages 1-2)).

Regarding claims 56 and 59, Wesinger further teaches the apparatus/method wherein at least one of said virtual machines provides at least a virtual central processor unit (0021-0023).

Regarding claims 57 and 60, Wesinger further teaches the apparatus/method, wherein at least one of said virtual machines is created using a virtual machine abstraction program (0012).

Regarding claims 58 and 61, Wesinger further teaches the apparatus/method, wherein at least one of said virtual machines is created using machine simulation/emulation software (0023-0028).

4. Claims 37-53 and 62-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wesinger, JR. et al. herein after (Wesinger) Pub. No. US 2001/0011304 A1 in view of Doran "Amdahl Multiple-Domain Architecture" Oct. 1988.

Regarding claim 37, Wesinger discloses a method of operating a real computer (fig. 1; *web server physical machine*) on behalf of plural customers (0012 lines 7-8, and 0050; *web users ... remote hosts*), the method comprising the step of:

operating plural virtual machines (fig. 1 *virtual host 1, 2, ... N*) on the real computer (fig. 1; *web server physical machine*), each of said plural virtual machines having a specification

specified by and configurable by a respective one of the customers in accordance with a computer service to be provided by the virtual machine on behalf of that customer (0035 and 0045-0053; *configuring multiple virtual hosts and/or client computers based on users preferences/budgets*).

Wesinger fails to disclose said at least one virtual machine having a separate operating system running thereon.

However Doran discloses running more than one operating system on a single computer in a virtual machine system (see page 22 col. 2-3).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Doran within the system of Wesinger because it would run different system control programs specialized for different applications, on a single computer and provide sufficient security in some application that the customer can avoid purchasing a special machine.

Regarding claim 38, Wesinger further teaches a method, comprising the step of operating plural virtual machines within the real computer for at least one of said customers (fig. 1; *web server physical machine and VH1... VHN*).

Regarding claim 39, Wesinger further teaches a method, comprising the step of operating a virtual network for at least one of said customers within the real computer, the or each virtual machine for said at least one customer being connected to said virtual network (0021-0027).

Regarding claim 40, Wesinger further teaches a method, comprising the step of using a virtual intrusion detection device for detecting an attack on the virtual network (The examiner takes an official notice on virtual intrusion detection as a well-known at the time of the invention was made because it would enable secure virtual network (see, Cisco News Release by San Jose pages 4-5).

Regarding claim 41, Wesinger further teaches a method, wherein at least one virtual machine is connected to a virtual firewall, the or each virtual firewall being connected to an external network to which customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall (0025).

Regarding claim 42, Wesinger further teaches a method, wherein the or each virtual machine for a particular customer is connected to a virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall being connected to an external network to which each of said customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall provided for that virtual machine or machines (0039).

Regarding claim 43, Wesinger further teaches a method, wherein each virtual firewall is set up within the real computer, the or each virtual machine for each customer being connected to a first port of the virtual firewall that is dedicated to that customer's virtual machine or machines, each

virtual firewall having a second port connected to a virtual network that is set up within the real computer and that is connected to an external network (0039).

Regarding claim 44, Wesinger further teaches a method, wherein the second port of each virtual firewall is connected to the same virtual network that is set up within the real computer and that is connectable to an external network (0025).

Regarding claim 45, Wesinger further teaches a method, wherein at least one virtual storage subsystem is provided and configured to allow multiple real data storage devices to emulate one or more virtual storage devices (0026).

Regarding claim 46, Wesinger further teaches a method, wherein the at least one virtual storage subsystem is configured to emulate at least one respective virtual storage device for each customer (0026).

Regarding claim 47, Wesinger further teaches a method, wherein a detection device is used for detecting evidence of malicious software or hostile attack signatures on the at least one virtual storage subsystem (0025).

Regarding claim 48, Wesinger further teaches a method, wherein the services provided include at least one of the services selected from: file, data and archiving services; applications hosting services; database hosting services; data warehouse services; knowledge management hosting

services; digital media production services; "intellectual property" and streaming media services; simple web hosting services; complex e-Commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services (0035).

Regarding claim 49, Wesinger further teaches a method, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between at least some of said virtual machines (0053).

Regarding claim 50, Wesinger further teaches a method, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between at least one virtual machine and an external computer (0021-0024).

Regarding claim 51, Wesinger further teaches a method, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between a first virtual network and a second virtual network (0053).

Regarding claim 52, Wesinger further teaches a method, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between a virtual network and an external computer (0021-0026).

Regarding claim 53, Wesinger teaches the method, comprising the step of moving said at least one virtual machine from a first real computer to a second real computer (The Examiner takes an official notice because to backup data during system failure the step of moving is necessary because it would recover data (see, Seagate software press releases 1997 pages 1-2)).

Regarding claim 62, Wesinger further teaches the apparatus/method wherein at least one of said virtual machines provides at least a virtual central processor unit (0021-0023).

Regarding claim 63, Wesinger further teaches the apparatus/method, wherein at least one of said virtual machines is created using a virtual machine abstraction program (0012).

Regarding claim 64, Wesinger further teaches the apparatus/method, wherein at least one of said virtual machines is created using machine simulation/emulation software (0023-0028).

5. Claims 54 and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wesinger, JR. et al. herein after (Wesinger) Pub. No. US 2001/0011304 A1 in view of Stewart et al. "The Motorola PowerPC TM PEEK profiler" 1997.

Regarding claim 54, Wesinger discloses an apparatus/method of providing for a plurality of customers (0012 lines 7-8, and 0050; *web users ... remote hosts*) one or more computer services selected from: file, data and archiving services; applications hosting services; database hosting services; data warehouse services; knowledge management hosting services; digital media

production services; "intellectual property" and streaming media services; simple web hosting services; complex e-Commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services (0035; *web hosting services*); the method comprising the steps of:

setting up on a real computer (fig. 1; *web server physical machine*) at the request of each of said customers (0024 and 0026; *user connection request to connect and access...*) at least one virtual machine (fig. 1 *virtual host 1, 2, ... N*) for each of said customers, said at least one virtual machine for each of said customers having a specification determined in accordance with the computer service or services requested by said customer and being configurable by said customer (0035 and 0045-0053; *configuring multiple virtual hosts and/or client computers based on users preferences/budgets*).

Wesinger fails to disclose said at least one virtual machine having a separate operating system running thereon.

However Stewart et al. discloses running multiple operating systems, like AIX TM, Mac TM OS, and Windows NT TM operating systems, on PowerPC processors (see abstract).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Stewart et al. within the system of Wesinger because they are analogous in service providing. One would have been motivated to incorporate the teachings of Stewart et al. because execute files under AIX, Mac OS and Windows NT.

Regarding claim 55, Wesinger further teaches the method, comprising the step of moving said at least one virtual machine from a first real computer to a second real computer (The Examiner

takes an official notice again because to backup data during system failure the step of moving is necessary because it would recover data (see, Seagate software press releases 1997 pages 1-2)).

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

March 20, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

3/20/07